

Dense Wavelength Division Multiplexed Quantum Key Distribution Using Entangled Photons

J. Mower,¹ F.N.C Wong,² J. H. Shapiro,² and D. Englund^{1,3}

¹*Department of Electrical Engineering, Columbia University, New York, NY 10027 USA*

²*Research Laboratory of Electronics, Massachusetts*

Institute of Technology, Cambridge, Massachusetts 02139

³*Department of Applied Physics and Applied Mathematics,
Columbia University, New York, NY 10027 USA*

Quantum key distribution (QKD) enables two parties to establish a secret key over a potentially hostile channel by exchanging photonic quantum states, relying on the fact that it is impossible for an eavesdropper to tap the quantum channel without disturbing these photons in a way that can be detected [1]. Here we introduce a large-alphabet QKD protocol that makes optimal use of temporal and spectral correlations of entangled photons, reaching the maximum number of independent basis states (the Schmidt number) and enabling extremely high information content per photon together with an optimal rate of secret key generation. This protocol, which we call ‘Dense Wavelength Division Multiplexed Quantum Key Distribution’ (DWDM-QKD), derives its security by the conjugate nature of the temporal and spectral entanglement of photon pairs generated by spontaneous parametric down conversion. By using a combination of spectral and temporal bases, we can adjust the protocol to be resource efficient. We show that DWDM-QKD is well suited to approach the optimal key generation rate using present-day sources, detectors, and DWDM optical networks from classical communications, as well as emerging optical interconnect and photonic integrated chip (PIC) systems.

There has been growing interest in QKD schemes employing photons in high dimensional Hilbert spaces, resulting in a potentially very large-alphabet size [1, 2]. Different degrees of freedom have been considered, including temporal [3, 4] and spatial modes [5]. Ultimately, the number of bits per photon is limited by the number of independent basis states spanning the Hilbert space, given by the Schmidt decomposition. While previous large-alphabet protocols in the temporal basis have reached up to 16 time bins [4] with a bit error rate of 5%, they were not able to reach the Schmidt number because, in practical situations, the detector timing jitter greatly exceeds the correlation time of entangled photons generated by typical spontaneous parametric down conversion (SPDC) sources. We overcome this limitation by employing temporal and spectral correlations simultaneously to match the performance of present-day detectors. Thus, given a certain detected-pair flux n and phase-matching bandwidth $\Delta\Omega$, the DWDM-QKD protocol proposed here allows two parties, Alice and Bob, to generate a secure key at the maximum rate possible in the time-frequency bases. In particular, DWDM-QKD enables Alice and Bob to generate their shared key at a maximum rate of $n \log_2(\Delta\Omega/n)$. Here, $\Delta\Omega/n$ corresponds to the maximum number of independent time-frequency states in time interval of duration $1/n$, and thus the maximum number of bits per photons is given by $\log_2(\Delta\Omega/n)$.

We consider time-frequency entangled photon pairs with a correlation time σ_{cor} produced by frequency-degenerate SPDC [6], assuming a pump field at frequency ω_p with coherence time σ_{coh} . In the weak pumping limit, the down-converted photon pair can be approximated by the state $|\Psi\rangle = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \psi(t_A, t_B) |t_A, t_B\rangle dt_A dt_B$, where $|t_A, t_B\rangle = \hat{a}_A^\dagger(t_A) \hat{a}_B^\dagger(t_B) |0\rangle$, and $\hat{a}_{A,B}^\dagger(t_j)$ denote the creation operators at time t_j for Alice and Bob, and $\psi(t_A, t_B)$ is the normalized time-domain biphoton wave function. This state can be written equivalently in the spectral domain, $|\Psi_\omega\rangle = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \psi(\omega_A, \omega_B) |\omega_A, \omega_B\rangle d\omega_A d\omega_B$, where $\psi(\omega_A, \omega_B) = \text{FT}_2\{\psi(t_A, t_B)\}$ and FT_2 denotes the two-dimensional Fourier transform. In these expressions, time and frequency represent conjugate

bases that can be employed to generate a secure key [2]. Specifically, we first discretize the biphoton state into n_t orthogonal temporal basis states, $|\sigma_{bin}^i\rangle$, of duration σ_{bin} , given by $|\sigma_{bin,A}^i, \sigma_{bin,B}^i\rangle = \int_{i\sigma_{bin}}^{(i+1)\sigma_{bin}} \int_{i\sigma_{bin}}^{(i+1)\sigma_{bin}} \psi(t_A, t_B) |t_A, t_B\rangle dt_A dt_B$, and alternatively into n_ω orthogonal spectral basis states, $|\nu^i\rangle$, of bandwidth $\delta\nu$, given by $|\nu_A^i, \nu_B^i\rangle = \int_{i\delta\nu}^{(i+1)\delta\nu} \int_{i\delta\nu}^{(i+1)\delta\nu} \psi(\omega_A, \omega_B) |\omega_A, \omega_B\rangle d\omega_A d\omega_B$. We assume $\sigma_{bin} > \sigma_{coh}$ and $\delta\nu > 1/\sigma_{coh}$. n_t and n_ω are bounded by the Schmidt number, $K = n_t n_\omega$.

In the protocol, Alice creates a biphoton pair, keeps one photon for herself, and sends the other photon to Bob. Alice and Bob randomly switch between measurements in the temporal ($n_t = K$, $n_\omega = 1$) and spectral ($n_t = 1$, $n_\omega = K$) bases at intervals of $T = 1/n$. After a certain time, they publicly compare their basis choices and divide their measurements into three categories, in which they (i) both detected photons and measured in the *same* basis set, (ii) both detected photons and measured in *different* basis sets, and (iii) did not both measure a photon. They discard category (iii) measurements. Type (i) measurements should be perfectly correlated, providing Alice and Bob with the raw sifted key. Eve does not know in which basis Alice and Bob are observing, and will therefore measure in the wrong basis set half of the time. If, for example, Alice and Bob do spectral measurements and Eve does a temporal measurement, she spreads the photon pair in frequency and increases the error probability in the type-(i) measurements, revealing her presence to Alice and Bob.

The use of two conjugate bases ensures security in the DWDM-QKD protocol. While measurements in these bases is practical for relatively small basis size, the demands on instruments become unrealistic for larger bases; for instance, generating the secure key at 10 bits per photon would require a minimum basis size of 1024, and therefore as many detectors (in a continuously running scheme). The temporal measurements present an additional challenge because typical SPDC sources at 1550 nm produce photon pairs with $\sigma_{coh} \sim 1$ ps for type-II phase-matched periodically poled KTiOPO₄ (PPKTP) ($\sigma_{coh} \sim 0.04$ ps for type-0 phase-matched periodically poled LiNbO₃ (PPLN)), which corresponds to a bandwidth of ~ 4 nm (~ 100 nm). No detector exists to measure such short time bins continuously [12]. This timing mismatch between practical detectors and practical sources implies that the realizable number of time bins $n_t < K$. When Alice and Bob measure in the temporal domain, they cannot check arrival temporal correlations to their fundamental limit. For instance, if the detector jitter is $\sigma_{det} \sim 30$ ps, as for SNSPD detectors [7], then $n_t/K \approx 1/30$, as indicated in the temporal measurement in Fig. 1a. As a result, Alice and Bob reduce the dimensionality of communication in the temporal domain from the Schmidt number [8], $K \approx \sigma_{coh}/\sigma_{coh}$ to $K' < \sigma_{coh}/\sigma_{det}$, and Eve can obtain finite spectral information without creating observable errors in the temporal basis. This example illustrates that in general, technological limitations reduce the number of basis states far below the fundamental limit.

To solve this problem, Alice and Bob can employ a hybrid basis that constitutes a superposition of temporal and spectral states. They measure in the temporal basis with resolution σ_{bin} and simultaneously in the spectral basis with resolution $(\sigma_{bin})^{-1}$. In this case, the maximum number of time bins becomes $n_t = \sigma_{coh}/\sigma_{bin}$ and the number of spectral bins becomes $n_\omega = \sigma_{bin}/\sigma_{coh}$ so that the total alphabet size becomes $n_t n_\omega = \sigma_{coh}/\sigma_{coh}$, which recovers the original Schmidt number, K . Now photons are measured in the spectral and temporal basis simultaneously, as shown in Figs. 1b and 1d.

The key generation rate depends on the phase-matching bandwidth, $\Delta\Omega$, and the number of photon pairs available for transmission. Alice and Bob can choose to transmit a single pair over this bandwidth, or can split the spectrum into some number of channels, N_c , each with photon flux, n/N_c . In both cases, the maximum key generation rate evaluates to

$$R \approx n \log_2 \left(\frac{\Delta\Omega}{n} \right). \quad (1)$$

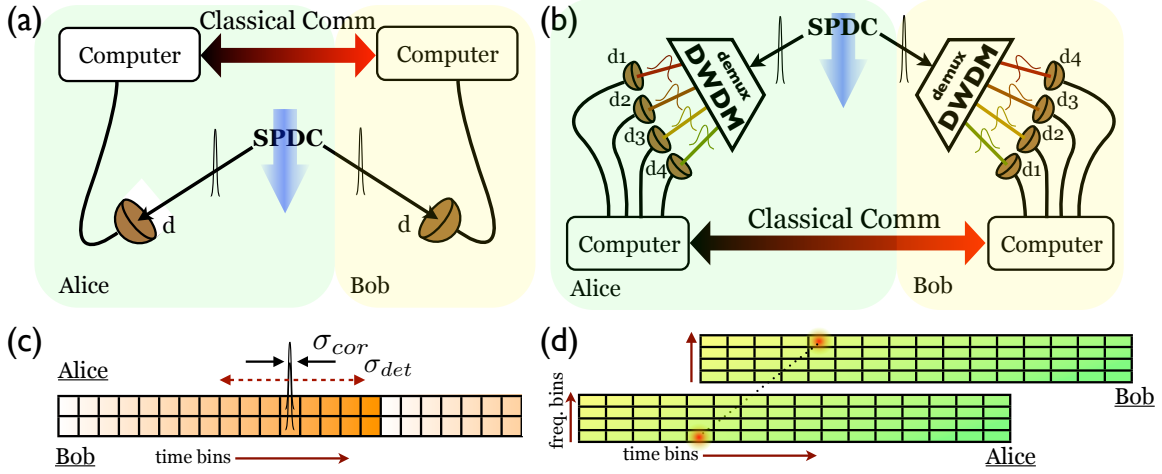


FIG. 1: (a) The temporal-coding scheme. A strong laser pumps a nonlinear crystal. Photon pairs are generated by SPDC and sent across channels of equal length to Alice and Bob who measure their arrival times. (b) Time bins agreed upon by Alice and Bob over a public channel. If a photon pair is detected in a given time bin, then that character is shared between Alice and Bob. (c) Alice and Bob place a DWDM before their detectors to obtain spectral information. (d) The new two-dimensional state space.

In Fig. 2a, we plot this relationship for two typical sources in the telecom band: a 1-cm type-II phase-matched PPKTP crystal generating photon pairs at 1550 nm with a 4 nm bandwidth; and a 2-cm type-0 phase-matched PPLN crystal at 1550 nm with a 100 nm bandwidth. Alice and Bob can generate a key at almost 20 bpp and 2 Gb/s using the PPLN source.

A careful analysis must take into account the finite overlap of the basis states. When we include this overlap as well as the detector timing jitter, we can calculate the mutual information between Alice and Bob as $I(A, B) = H(A) + H(B) - H(A, B)$, using the Shannon entropy, $H = -\sum_{\{x\}} p^{\{x\}} \log p^{\{x\}}$, where $\{x\}$ is the complete set of indices spanning a probability density function p . We evaluate $I(A, B)$ in Appendix II A and plot the results in Fig. 2b, as a function of the number of Gaussian spectral channels, and the number of time bins. We use Gaussian channels to approximate modern DWDM filters. The continuous lines represent the ideal information per photon, and the data points represent our simulated results for the mutual information using a two-dimensional Gaussian, $\psi(t_A, t_B) \propto e^{-(t_A - t_B)^2 / 4\sigma_{cor}^2} e^{-(t_A + t_B)^2 / 4\sigma_{coh}^2} e^{-i\omega_p(t_A + t_B)/2}$, for the biphoton wave function, where ω_p is the pump frequency. For a small number of spectral channels, we see good agreement. For large numbers, the Gaussian filters slightly underperform the ideal result due to crosstalk in the closely spaced temporal and spectral bins. This is evident in Fig. 2b for 32 spectral channels with FWHM of $(n_\omega \sigma_{cor})^{-1}$ and channel spacing $4(n_\omega \sigma_{cor})^{-1}$, and two 40 ps time bins.

Our formalism also enables us to study the effect of detector timing jitter. The results are plotted in the inset in Fig. 2b and show that the mutual information drops rapidly when the timing jitter approaches the time bin duration.

The security check employing conjugate bases in purely frequency and time relies on the mutually unbiased nature of these bases; a measurement in the wrong basis reveals no information about the state in the other basis and by their conjugate nature introduces errors. We therefore seek a mutually unbiased basis to that employed in our resource-efficient scheme. Alice and Bob's coarse

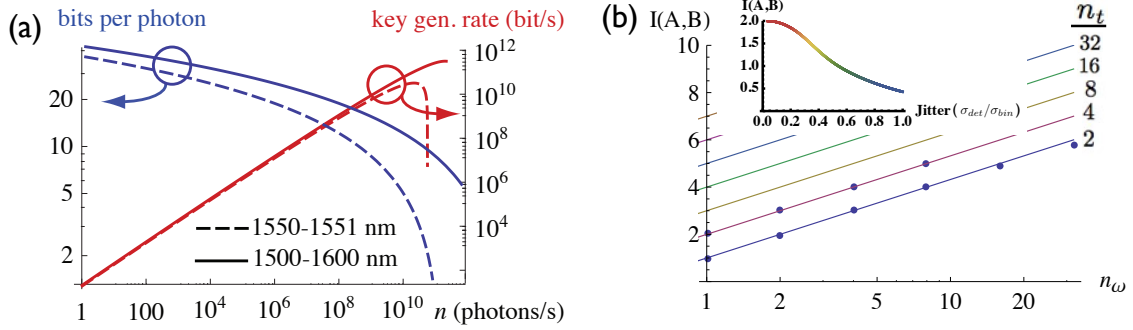


FIG. 2: (a) Key exchange rate and bits per photon as a function of phase-matching bandwidth and photon flux. (b) Mutual information as a function of the number of spectral channels, n_ω . The individual spectral channels have bandwidth $\delta\nu = \Delta\omega/n_\omega$ and spacing $4\delta\nu$. Increasing the number of spectral channels increases the bits per photon, until the time duration of the filtered photon approaches σ_{bin} . The inset shows mutual information as a function of detector timing jitter, σ_{det} , normalized to σ_{bin} .

measurements in spectrum are described by an operator that projects subsets of spectral states onto degenerate eigenvalues Ω_l . The degeneracy within these subsets is lifted by also performing measurements in time, which are described by an operator with coarse timing resolution T_m that correspond to degenerate sets of eigenstates. Simultaneous eigenstates for time and spectral measurements $|\Omega_l T_m\rangle$ describe one basis set. A conjugate basis can be found that forms the second basis for measurements by Alice and Bob.

Under certain conditions, a security check can be performed using simple instrumentation. For now, we assume that Eve chooses to attack by using either a Gaussian envelope in time or one in frequency, i.e., $\hat{E}_t = \int_{-\infty}^{\infty} e^{-t^2/2(\sigma_{coh}^E)^2} |t\rangle \langle t| dt$ [4] or $\hat{E}_\omega = \int_{-\infty}^{\infty} e^{-(\sigma_{cor}^E)^2(\omega-\omega_p/2)^2} |\omega\rangle \langle \omega| d\omega$, respectively. Eve's temporal measurement leads to a decrease in σ_{coh} , and her frequency measurement creates an increase in the biphoton correlation time, σ_{cor} . Alice and Bob can detect both of these attacks with the 'extended Franson interferometer' (eFI) shown in Fig. 3. The eFI is composed of two unbalanced Mach-Zehnder interferometers (MZI) in the possession of Alice and Bob, where the long path on one arm can be actively modulated.

The probability for Alice and Bob to detect a photon coincidence in their eFI is [9]

$$P_C \propto \frac{1}{2} + \frac{1}{2} \cos[\omega(2\Delta t - \delta t)] e^{-\delta t^2/8\sigma_{cor}^2} e^{-\Delta t^2/8\sigma_{coh}^2}, \quad (2)$$

where $\omega = \omega_p/2$ is the center frequency of the SPDC signal and idler photons, Δt is the path-length difference between the long and short arm of Alice's MZI, and δt is the path-length difference between Alice's and Bob's long arm. Δt is large enough to avoid single photon interference between long and short paths of a single arm of the eFI, and δt is varied on the order of $1/\omega$ about zero. The interference is plotted in Fig. 3 as a function of an additional delay in Alice's MZI. This interference curve shows the oscillations in P_C that is typical of the Franson interferometer near $\delta t = 0$. In addition, this oscillation has a Gaussian envelope whose width is given by σ_{cor} .

The visibility of the eFI interference is $V = e^{-\delta t^2/8\sigma_{cor}^2} e^{-\Delta t^2/8\sigma_{coh}^2}$. If Eve measures in the temporal domain with a resolution better than Δt , then Alice and Bob can detect a drop in V near $\delta t = 0$; this is the security check used by Kahn *et. al* in Ref. [4]. On the other hand, if Eve measures in the spectral domain with a resolution better than $\Delta\Omega$, then Alice and Bob can detect

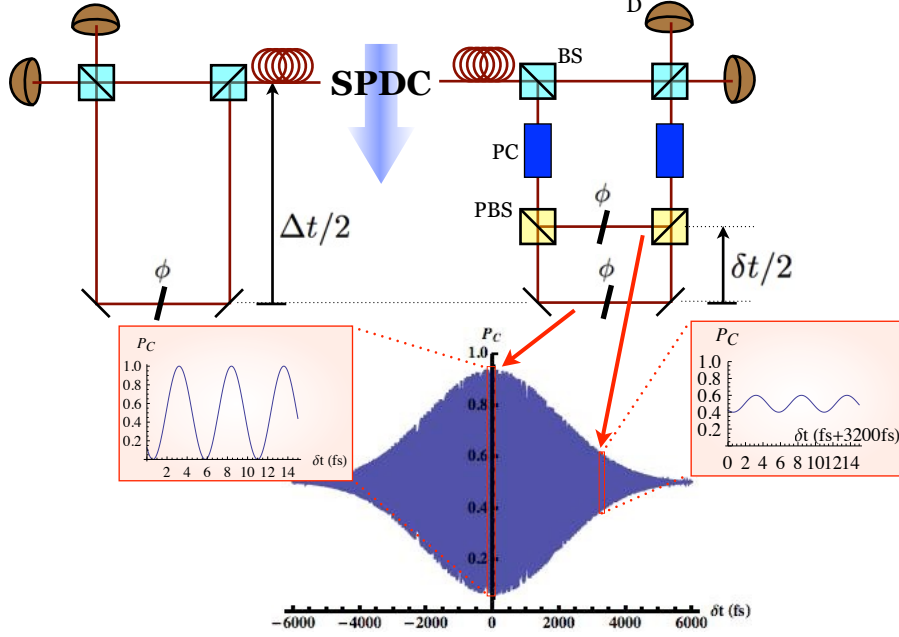


FIG. 3: The eFI used for security checks. Alice switches the short arm of her Franson between lengths δt_1 and δt_2 . This allows determination of both σ_{coh} and σ_{cor} so that weak spectral and temporal measurements on the photon pair can be detected. Alice and Bob do security checks by varying δt as shown in the insets. We show one possible switching scheme that makes use of Pockels cells (PC) to rotate the polarization of the photon by $\pi/2$ so that it is either transmitted or reflected at the polarizing beam splitter (PBS) and sent to the extended or standard delay line, respectively. The eFI also includes non-polarizing beam splitters (BS) and single photon detectors (D).

an increase in V near $\delta t = \sigma_{cor}$. To guard against temporal and spectral measurements by Eve simultaneously, Alice and Bob measure V while Alice switches randomly between delays of 0 and σ_{cor} (see Fig. 3).

Alice and Bob can deduce the correlation time and coherence time from two visibility measurements V_1 and V_2 using two delays, δt_1 and δt_2 , respectively. We label these extrapolated values $\sigma_{coh}^{E'}$ and $\sigma_{cor}^{E'}$, which are given by

$$(\sigma_{cor}^{E'})^2 = \frac{1}{8} \frac{\delta t_1^2 - \delta t_2^2}{\ln V_2 - \ln V_1} \quad (3)$$

$$(\sigma_{coh}^{E'})^2 = \frac{1}{8} \frac{\Delta t^2 (\delta t_1^2 - \delta t_2^2)}{\delta t_1^2 \ln V_2 - \delta t_2^2 \ln V_1}. \quad (4)$$

Using $(\sigma_{coh}^E)^2 = 1/[(\sigma_{coh}^{E'})^{-2} - \sigma_{coh}^{-2}]$ and $(\sigma_{cor}^E)^2 = 1/[(\sigma_{cor}^{E'})^{-2} - \sigma_{cor}^{-2}]$ derived from this measurement, the bound on Eve's information per photon is $I_E \leq \log_2(\sigma_{coh}/\sigma_{coh}^{E'}) + \log_2(\sigma_{cor}^E/\sigma_{cor}^{E'})$, which is the sum of her information obtained from temporal and spectral measurements. Our assumption of a Gaussian form of Eve's POVM will be generalized in future work.

I. CONCLUSION

The often limited photon budget for quantum key distribution makes high-dimensional encoding desirable. However, achieving the limit on this dimensionality in the temporal domain using time-frequency entangled photon pairs requires detectors with sub-ps timing jitter and resolution. By invoking conjugate spectral correlations, we present a protocol to approach this fundamental limit using current detectors and existing telecom networks. The conjugate nature of temporal and spectral encoding means that one can trade spectral for temporal bits (and vice versa) to minimize the effect of channel distortion such as nonlinear frequency conversion and dispersion, in addition to optimizing over transmission rate and channel bandwidth.

This work was supported by the DARPA Information in a Photon program, through grant W911NF-10-1-0416 from the Army Research Office.

II. METHODS

A. Mutual information

Alice and Bob ideally communicate information by discretizing the wave function into agreed-upon time-bin $|\sigma_{bin}^i\rangle$ and frequency-bin $|\nu^i\rangle$ macrostates by

$$|\bar{\Psi}\rangle = \sum_{i,j,k,l} G^{i,j,k,l} |\sigma_{bin,A}^i, \sigma_{bin,B}^j, \nu_A^k, \nu_B^l\rangle, \quad (5)$$

where

$$G^{ijkl} = \int_{i\sigma_{bin}}^{(i+1)\sigma_{bin}} \int_{j\sigma_{bin}}^{(j+1)\sigma_{bin}} \text{FT}_2 \left[\int_{k\delta\nu}^{(k+1)\delta\nu} \int_{l\delta\nu}^{(l+1)\delta\nu} \psi(\omega_A, \omega_B) d\omega_A d\omega_B \right] dt_A dt_B \quad (6)$$

. The probability of Alice and Bob projecting into time bins $|\sigma_{bin,A}^i\rangle$ and $|\sigma_{bin,B}^j\rangle$ and frequency bins $|\nu_A^k\rangle$ and $|\nu_B^l\rangle$ is $p^{i,j,k,l} = |\langle \sigma_{bin,A}^i, \sigma_{bin,B}^j, \nu_A^k, \nu_B^l | \bar{\Psi} \rangle|^2 = |G^{i,j,k,l}|^2$. We label the frequency bins so that for $k = l$, the center frequencies of these bins add to the pump frequency. We plot the mutual information in Fig. 2b as a function of the number of spectral channels added. The wave function is a two-dimensional Gaussian. As we increase the number of spectral channels, the mutual information (MI) increases, however the timing correlations eventually start to decrease, as the filtered photons extend into neighboring time bins. Jitter is also a very important to the MI calculation. We include this in the inset to Fig. 2b.

B. Detector timing jitter

Detector timing jitter refers to the added uncertainty in the photon detection time of some stimulus, purely a result of detector electronics. Superconducting nanowire single photon detectors and InGaAs APDs both exhibit jitter of roughly 30 to 40 ps [10]. We model timing jitter as a Gaussian projection, $\hat{\sigma}_{det} = \int e^{-t_x^2/2\sigma_{det}^2} |t\rangle \langle t + t_x| dt_x$. The jitter profile of a real photodetector is not truly Gaussian and can be quite asymmetric, however (1) this model allows for first-order

analysis and (2) certain single photon detectors do have approximately Gaussian timing jitter [7]. If we apply $\hat{\sigma}_{det}$ on both Alice and Bob's photons, assuming the two-dimensional Gaussian given earlier, we get

$$\hat{\sigma}_{det,A}\hat{\sigma}_{det,B}|\Psi\rangle \propto \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \exp\left[\frac{-(t_A+t_B)^2}{4\sigma_{det}^2+16\sigma_{coh}^2}\right] \exp\left[\frac{-(t_A-t_B)^2}{4\sigma_{det}^2+4\sigma_{cor}^2}\right] e^{i\omega_p(t_A+t_B)/2} |t_A, t_B\rangle dt_A dt_B \quad (7)$$

Since $\sigma_{coh} \gg \sigma_{det}$, the most important effect of jitter is to increase the observed correlation time roughly from σ_{cor} to σ_{det} . This can have a significant effect on the mutual information between Alice and Bob if σ_{det} is on the order of σ_{bin} , as shown in Fig. 2b.

III. SUPPLEMENTARY INFORMATION

A. Lossy Franson interferometry

The Franson interference derived in the text assumes lossless propagation through the interferometer. This assumption is not valid in photonic integrated chips or fiber networks. We can account for loss in our analysis by adding a virtual beam splitter in the long path of the otherwise-lossless Franson, which couples the waveguide mode with a vacuum mode (see Fig. 4). We work in the Heisenberg construction, evolving the annihilation operator through the virtual-loss beam splitter and the two Franson beam splitters. The matrix for beam splitters 1 and 2, which leave the third mode undisturbed is given by

$$\hat{U}_i = \begin{pmatrix} \sqrt{r_i} & \sqrt{1-r_i} & 0 \\ \sqrt{1-r_i} & -\sqrt{r_i} & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (8)$$

where $i \in 1, 2$. The virtual-loss beam splitter is given by

$$\hat{U}_L = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{t_L} & \sqrt{1-t_L} \\ 0 & \sqrt{1-t_L} & -\sqrt{t_L} \end{pmatrix} \quad (9)$$

The resulting annihilation operators are then $\hat{a}_A(t_A) = C_1\hat{a}(t) + C_2\hat{a}(t - \Delta t)$ and $\hat{a}_B(t_B) = C_1\hat{a}(t) + C_2\hat{a}(t - \Delta t - \delta t)$, disregarding the vacuum term, which will not affect coincidence counting. $C_1 = \sqrt{r_1}\sqrt{r_2}$ and $C_2 = \sqrt{1-r_1}\sqrt{1-r_2}\sqrt{t_L}$. For $r_1 = r_2 = 1/2$, and $t_L = e^{-2t/\tau_\alpha}$ where τ_α is the lifetime of the photon in the interferometer arm, the visibility simplifies to

$$V_{PIC} = \frac{2e^{-2\Delta t/\tau_\alpha}}{1 + e^{-4\Delta t/\tau_\alpha}} e^{-\delta t^2/2\sigma_{cor}^2} e^{-\Delta t^2/2\sigma_{coh}^2}. \quad (10)$$

However for maximum visibility, $C_1 = C_2$, so

$$\frac{\sqrt{r_1}\sqrt{r_2}}{\sqrt{1-r_1}\sqrt{1-r_2}} = \sqrt{t_L}. \quad (11)$$

The Franson beam splitters can therefore be tuned to account for loss in the interferometer.

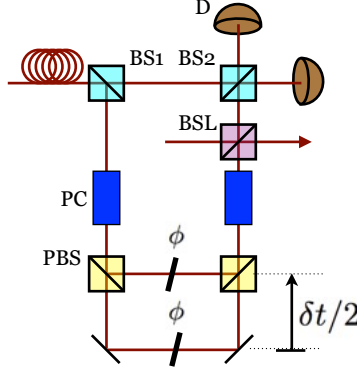


FIG. 4: The eFI with an additional virtual beam splitter for loss in the long arm.

B. Eve and the wave function

We focus on the case of a single eavesdropper measuring a single photon of the photon pair. Eve's temporal measurement is a Gaussian filtering function

$$\hat{E}_t = \int_{-\infty}^{\infty} e^{-t^2/2(\sigma_{coh}^E)^2} |t\rangle \langle t| dt \quad (12)$$

Following [4], the amplitude function

$$\psi(t_A, t_B) \propto \exp[-(t_A - t_B)^2/4\sigma_{cor}^2] \exp[-t_A^2/4\sigma_{coh}^2] e^{i\omega_p(t_A+t_B)/2}, \quad (13)$$

for $\sigma_{coh} \gg \sigma_{cor}$. Therefore

$$\begin{aligned} |\Psi_E\rangle &= \hat{E}_t |\Psi\rangle \\ &\propto \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \exp\left[-t_A^2 \left(\frac{1}{4\sigma_{coh}^2} + \frac{1}{4(\sigma_{coh}^E)^2}\right)\right] \exp\left[\frac{-(t_A - t_B)^2}{4\sigma_{cor}^2}\right] e^{i\omega_p(t_A+t_B)/2} |t_A, t_B\rangle \end{aligned} \quad (14)$$

so the coherence time of the biphoton packet is strongly influenced by Eve's timing resolution when $\sigma_{coh}^E \ll \sigma_{coh}$. Similarly, we define a weak spectral POVM,

$$\hat{E}_\omega = \int_{-\infty}^{\infty} e^{-(\sigma_{cor}^E)^2(\omega - \omega_p/2)^2} |\omega\rangle \langle \omega| d\omega \quad (15)$$

For $1/\sigma_{cor} \gg 1/\sigma_{coh}$, $|\Psi\rangle$ can be written in the spectral-domain representation as follows

$$|\Psi\rangle \propto \int \int \exp[-\sigma_{cor}^2/4(2\omega_A - \omega_p)^2] \exp[-\sigma_{coh}^2(\omega_A + \omega_B - \omega_p)^2] |\omega_A, \omega_B\rangle d\omega_A d\omega_B, \quad (16)$$

from which we find that

$$\begin{aligned} \hat{E}_\omega |\Psi\rangle &\propto \int \int \exp[-(\sigma_{cor}^2/4 + (\sigma_{cor}^E)^2/4)(2\omega_A - \omega_p)^2] \\ &\quad \times \exp[-\sigma_{coh}^2(\omega_A + \omega_B - \omega_p)^2] |\omega_A, \omega_B\rangle d\omega_A d\omega_B. \end{aligned} \quad (17)$$

Thus, Eve projects the biphoton pair onto a narrower frequency distribution. Reverting to the time-domain representation we get

$$\hat{E}_\omega |\Psi\rangle \propto \int \int \exp(-t_A^2/4\sigma_{coh}^2) \exp[-(t_A - t_B)^2/4(\sigma_{cor}^E)^2] e^{i\omega_p(t_A+t_B)/2} |t_A, t_B\rangle dt_A dt_B, \quad (18)$$

for $\sigma_{cor} \ll \sigma_{cor}^E \ll \sigma_{coh}$.

-
- [1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
 - [2] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
 - [3] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
 - [4] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. **98**, 060503 (2007).
 - [5] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, Nature Physics **4**, 282 (2008).
 - [6] Y. H. Shih and C. O. Alley, Phys. Rev. Lett. **61**, 2921 (1988).
 - [7] E. Dauler, B. Robinson, A. Kerman, J. Yang, E. Rosfjord, V. Anant, B. Voronov, G. Gol'tsman, and K. Berggren, Applied Superconductivity, IEEE Transactions on **17**, 279 (2007).
 - [8] C. K. Law and J. H. Eberly, Phys. Rev. Lett. **92**, 127903 (2004).
 - [9] J. D. Franson, Phys. Rev. Lett. **62**, 2205 (1989).
 - [10] R. H. Hadfield, Nature Photonics **3**, 696 (2009).
 - [11] M. A. Foster, R. Salem, D. F. Geraghty, A. C. Turner-Foster, M. Lipson, and A. L. Gaeta, Nature **456**, 81 (2008).
 - [12] Time-lens approaches [11] may be used to stretch time by some factor N_{TL} , but this requires the protocol to be run in bursts so that neighboring intervals do not overlap; up-conversion detectors can offer very short timing resolution, but introduce too many dark counts in the continuously running protocol